

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including the formulation of policies to effectuate the purposes of the agency (A.R.S. § 41-3504(A (13))).

2. PURPOSE

To provide technology and security requirements for Virtual Office (VO) client devices enabling state personnel to work from home or from some other designated location approved by Budget Units. Virtual Office initiatives and programs will further enable and improve business continuity activities, organizational agility, and further help retain top talent within state government.

3. SCOPE

This applies to all budget units. A budget unit is defined as a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona board of regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. POLICY

Virtual Office (VO) activities are a strategic initiative for the mobility of state personnel that is expected to increase considerably over the next few years. All other policies and procedures related to VO alternative work arrangements through management readiness, operational reviews, education, and pilot proposals can be located in the VO Toolkit¹ as implemented by the Governor's Office of Efficiency Review.

4.1 Technical Requirements

Budget Units that comply with the state's Enterprise Architecture Policies and Standards² on platform, software, network, data/information, and security will

¹ <http://www.teleworkarizona.com/vo/Toolkit.doc>

² <http://www.azgita.gov/policies%5Fstandards/>

have a greater selection and choice of VO client devices and software for state personnel (i.e., thin vs. thick clients).

- 4.1.1 Budget Units shall perform a technology assessment on VO client devices to establish a standard based on deployed technical security schemes/programs and IT infrastructure. Please refer to the VO toolkit.³
- 4.1.2 VO connections for upload and download speeds from an Internet Service Provider (ISP) shall be determined and based on the business needs of the Budget Unit, estimated volumes of traffic, and bandwidth.
- 4.1.3 It is recommended that multiple dual-core servers should be used to load-balance connections equally and be geographically dispersed for scalability in the event a budget unit has more than fifty (50) VO client devices.
- 4.1.4 All VO devices will verify utilize the state network and therefore shall comply with all statewide IT policies and standards. Please refer to GITA's web-site on statewide standards.²

4.2 Security Requirements

Security is a concern for the state when Budget Units participate in VO activities because of the possibility of backdoor cyber intrusions that may affect the state network, infrastructure, and data/information. Therefore, the following security requirements shall be deployed when approving VO for state employees and contractors (participants):

- 4.2.1 A secure VPN tunnel shall be deployed for all VO clients and connected/routed through the AZNET network which provides centralized security architecture for the state. AZNET will ensure all VO traffic is analyzed for unauthorized access, traffic, and hostile threats to further secure and protect information assets of the state. For additional information please refer to Statewide Standard S830, Network Security.⁴
- 4.2.2 Firewall software shall be deployed, activated and set at a medium/high setting for each VO device. For additional information please refer to Statewide Standard P800-S830, Network Security.⁴
- 4.2.3 Should Budget Units permit Internet access for VO client devices it shall be provided via a back-haul⁵ to ensure agency firewall and filtering capabilities are functional in protecting state VO resources.
- 4.2.4 Two factor authentication is recommended. For additional information please refer to Statewide Standard P800-S820, Authentication and Directory Services.⁶

³ <http://www.teleworkarizona.com/vo/Toolkit.doc>

⁴ http://www.azgita.gov/policies_standards/word/P800-S830%20Network%20Security%20Std%20r2.doc

⁵ Back Haul – refers to transmitting from a remote site or network to a central or main site.

⁶ http://www.azgita.gov/policies_standards/word/P800-

- 4.2.5 All Budget Units participating in VO programs shall deploy the use of encryption and protection techniques for the transmission and storage of confidential data/information over state networks. For additional information please refer to Statewide Standard P800-S850, Encryption Technology.⁷
- 4.2.6 VO client devices shall deploy and activate industry standard malware (antivirus and spyware) software programs to mitigate potential software problems. For additional information please refer to Statewide Standard P800-S860, Virus and Malicious Code Protection.⁸
- 4.2.7 VO client devices shall not be configured with an unsecured wireless network. IEEE 802.11x security software shall be deployed in addition to enabling all security and encryption features of a wireless network. For additional information please refer to Statewide Standards P800-S830 Network Security and P800-S850 Encryption Technologies.⁹
- 4.2.8 VO client devices shall not participate in any personal in-home network of a VO participant unless all networked devices within the personal network comply with this policy and referenced standards.
- 4.2.9 It is recommended that all software applications accessed by VO client devices be accessed from Budget Unit server(s) and not from a VO client.
- 4.2.10 It is at the discretion of the Budget Unit as to whether systems software, software applications, and productivity software other than state owned software are allowed on VO client devices.
- 4.2.11 All data retrieved and stored should be accessed from a Budget Unit storage device (DAS, NAS, SAN) and not from a VO client. This is at the discretion of the Budget Unit based on deployed secure authentication and authority schemes as well as trusted source.
- 4.2.12 Printing from a VO client, storing data on VO local storage or copying to local storage is at the discretion of the Budget Unit based on deployed secure authentication and authority schemes as well as trusted source.
- 4.2.13 All hard copy reports printed from a VO client that has satisfied a business decision and/or state requirement with no further apparent value or importance shall be shredded or incinerated.
- 4.2.14 Should a VO participant ever lose possession or control of a VO client, or lose a hard copy report with confidential information, an **Incident Report** shall immediately be submitted to the Statewide Infrastructure Protection Center (SIPC) of ADOA.¹⁰

⁷ [S820%20Authentication%20and%20Dir%20Svcs%20std.doc](http://www.azgita.gov/policies_standards/word/P800-S850%20Encryption%20Technologies%20Standard%20r2.doc)

⁸ http://www.azgita.gov/policies_standards/word/P800-S860%20Virus%20Protection%20Std%20r3.doc

⁹ http://www.azgita.gov/policies_standards/word/P800-S850%20Encryption%20Technologies%20Standard%20r2.doc

¹⁰ <http://www.azdoa.gov/isd/ais/state-infrastructure-protection-center>

- 4.2.15 Should a VO client be disposed of, sold, or gifted by a participant, the participant shall clean and sanitize local storage devices according to S880 Media Sanitizing/Disposal standard.¹¹
- 4.2.16 Should a VO participant quit or be terminated from state employment or state contract, the Budget Unit shall immediately clean and sanitize all related VO local storage devices of all state data/information according to S880 Media Sanitizing/ Disposal standard.¹²
- 4.2.17 Budget Units shall comply with Statewide Standard P800-S870, Backups¹³ for all data access and update activities from VO client devices.
- 4.2.18 VO client devices shall be plugged into a resettable power-surge protector to safeguard hardware and software in the event of electrical problems.

4.3 Administrative

- 4.3.1 It is at the Budget Unit's discretion to fund VO client device(s) or portions thereof, or have state participants responsible for VO costs.
- 4.3.2 The state reserves the right to digitally scan VO clients and storage devices with or without notice.
- 4.3.3 All Budget Units have the right to develop additional VO policies, standards, and/or procedures compliant with this policy.
- 4.3.4 All VO participants are required to sign a VO Non-Disclosure Agreement. See Attachment A, Sample of a Virtual Office (VO) Non-Disclosure Agreement.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

- 6.1 A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
- 6.2 A. R. S. § 41-761 et seq., "Personnel Administration."
- 6.3 A. R. S. § 41-770, "Causes for dismissal or discipline."
- 6.4 A. R. S. § 41-1335 ((A (6 & 7))), "State Agency Information."
- 6.5 A. R. S. § 41-1339 (A), "Depository of State Archives."
- 6.6 A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
- 6.7 A. R. S. § 41-3501, "Definitions."
- 6.8 A. R. S. § 41-3504, "Powers and Duties of the Agency."

¹¹ http://www.azgita.gov/policies_standards/word/P800-S880%20Media%20Sanitize%20Disposal%20Std%20r2.doc

¹² http://www.azgita.gov/policies_standards/word/P800-S880%20Media%20Sanitize%20Disposal%20Std%20r2.doc

¹³ http://www.azgita.gov/policies_standards/word/P800-S870%20Backups.doc

- 6.9 A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
- 6.10 A. R. S. § 44-7041, "Governmental Electronic Records."
- 6.11 Arizona Administrative Code, Title 2, Chapter 5, "Department of Administration, Personnel Administration.
- 6.12 Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
- 6.13 Arizona Administrative Code, Title 2, Chapter 11, Article 3, "Solicitation" (A.A.C. R2-11-309).
- 6.14 Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
- 6.15 ADOA Telework Policy - <http://www.azdoa.gov/publications-1/telework-program.pdf/view?searchterm=telework>
- 6.16 Virtual Office Implementation Toolkit -
<http://www.teleworkarizona.com/vo/Toolkit.doc>
- 6.17 [Statewide Policy P100, Information Technology.](#)
- 6.18 [Statewide Policy P252, Intellectual Property and Fair Use.](#)
- 6.19 [Statewide Policy P800, IT Security.](#)
- 6.20 [Statewide Standard P800-S820 Authentication and Directory Services Standard.](#)
- 6.20 [Statewide Standard P800-S830, Network Security.](#)
- 6.21 [Statewide Standard P800-S850, Encryption Technologies.](#)
- 6.22 [Statewide Standard P800-S860, Virus and Malicious Code Protection.](#)

7. ATTACHMENTS

Attachment A – Sample Virtual Office (VO) Non-Disclosure Agreement

Attachment A. Sample

Virtual Office (VO) Non-Disclosure Agreement

I, _____, have read and understand the
Print Name

P150 Virtual Office Policy. I agree to comply with conditions of this standard and agree that the State of Arizona reserves the right to monitor and log all Virtual Office VPN network activity without notice.

I agree that all Virtual Office client devices and software purchased by the State remain the property of the State of Arizona and that I have no expectation of privacy in the use of these resources while participating in State Virtual Office activities.

I agree that all Virtual Office client devices and/or portions thereof purchased by state employees and/or contractors shall remain the property of the individual employee/contractor and each shall have no expectation of privacy in the use of these resources while participating in State Virtual Office activities.

I agree that all state data/information residing on Virtual Office client devices, whether public or confidential, shall remain the property of the State of Arizona.

I agree that the State reserves the right to cancel my Virtual Office privileges at any time.

Signed: _____ Date: _____

LIABILITY

Neither the State of Arizona nor the _____
(Agency Name)
make warranties of any kind, whether express or implied, for the use of Virtual Office client devices or other VO electronic resources. Additionally, neither the State of Arizona nor the agency indicated above is responsible for any damages, whatsoever, that Virtual Office participants may suffer arising from or related to the use of Virtual Office client devices and other Virtual Office electronic resources.